ECS Configuration Change Request

1. Originator	2. Log Date:	3. CCR #:	4. Rev:	5. Tel:	6. Rm #:	7. Dept.
Robert Cole	7/18/02	02-0598	-	301-925-0799	2110C	SE/HW

8. CCR Title: Submit Test Executable to upgrade Axis firmware for security vulnerabilities

9. Originator Signature/Date	10. Class	11. Type:	12. Need Date: 7/19/02
/s/ Robert Cole 7/18/02	II	CCR	

13. Office Manager Signature/Date	14. Category of Change:	15. Priority: (If "Emergency" fill in Block 27).
/s/ James R. Mather 7/18/02	Update ECS Baseline Doc.	Emergency

16. Documentation/Drawings Impacted:	17. Schedule Impact:	18. CI(s) Affected: DIPHW
N/A		

19. Release Affected by this Change:	20. Date due to Customer:	21. Estimated Cost:
N/A		None - Under 100K

22. Source Reference: ☒ NCR (attach) ☐ Action Item ☐ Tech Ref. ☐ GSFC ☐ Other:
ECSed34495

23. Problem: (use additional Sheets if necessary)
Security vulnerabilities exist under the current configuration and firmware level of the Axis print server which is used with the Internem label printers in PDS. The following vulnerabilities have been identified by the ISS security scan:
SNMPv1 trap or request handling
SNMP_Set guessed community name and changed system information
FTP daemon with no password
SNMP_Set used public community name to change system information

24. Proposed Solution: (use additional sheets if necessary)
Issue the attached Test Executable to resolve these vulnerabilities. The attached sheet details the procedure to upgrade the Axis firmware and make the necessary configuration changes. This will be released as patch ISS.01

Distribute the firmware file 54xp.bin to all sites. The cksum output for this file is:
1876557108 1160501 54xp.bin

25. Alternate Solution: (use additional sheets if necessary)
Accep the risk associated with the above vulnerabilities.

26. Consequences if Change(s) are not approved: (use additional sheets if necessary)

27. Justification for Emergency (If Block 15 is "Emergency"):
NCR ECSed34495 is at severity level 2. This issue is currently ranked at 15 in the OPS priority list.

28. Site(s) Affected: ☐ EDF ☒ PVC ☒ VATC ☒ EDC ☒ GSFC ☒ LaRC ☒ NSIDC ☐ SMC ☐ AK ☐ JPL ☐ EOC ☐ IDG Test Cell ☐ Other

29. Board Comments:	30. Work Assigned To:	31. CCR Closed Date:

32. EDF/SCDV CCB Chair (Sign/Date): /s/ Byron V. Peters 7/18/02	**Disposition:** Approved App/Com. Disapproved Withdraw Fwd/ESDIS ERB Fwd/ECS
33. M&O CCB Chair (Sign/Date): s/s Pamela Johnson 7/18/02	**Disposition:** Approved App/Com. Disapproved Withdraw Fwd/ESDIS ERB Fwd/ECS
34. ECS CCB Chair (Sign/Date):	**Disposition:** Approved App/Com. Disapproved Withdraw Fwd/ESDIS ERB Fwd/ESDIS

ADDITIONAL SHEET

CCR #: 02-0598 **Rev: - Originator:** Rob Cole

Telephone: **Office:**

Title of Change: Submit Test Executable to Upgrade Axis Firmware for Security Vulnerabilities

Issue: Several security vulnerabilities have been identified with the current Intermec label printer and Axis print server configuration in the PDS subsystem:

SNMPv1 trap or request handling
SNMP_Set guessed community name and changed system information

SNMP_Set used public community name to change system information

Fix: The following actions should be completed to resolve the above vulnerabilities:

Upgrade Axis Firmware:
An upgrade to version 6.0 of the Axis 540+ print server firmware will resolve the SNMPv1 trap or request handling vulnerability.

1. Obtain a copy of the file 54xp.bin. This file will be distributed to the DAACs via the Configuration Management software distribution process.
2. Connect to the Axis print server using FTP and login as root.
3. Enter binary at the FTP prompt to change to binary mode transfer
4. Enter put 54xp.bin flash to upload the new firmware to the print server.

After the file in transferred, the print server will automatically restart running the new firmware

Modify Configuration File

Modifications to the Axis configuration file will resolve the other vulnerabilities.

1. Download the Axis configuration file to a host computer.

Login to the print server using the command ftp IP_ADDR where IP_ADDR is the IP address of the print server. Enter root at the user id prompt and pass at the password prompt.
Download the configuration file from the print server using the command get config.
2. Edit the configuration file

Change the 3rd and 4th lines in the General menu to the following:
ROOT_PWD. : <root_pwd>
USERS. : u:<user_name>:p:<user_pwd>

Note: The root and user passwords chosen for the above lines can be the same. Ensure that passwords are at least eight characters and contain an uppercase letter, number and special character among the first 8 characters.

Change the 1st, 2nd, 4th and 5th lines in the SNMP menu to the following:
READ_COM : <snmp_pwd>
WRT_COM. : <snmp_pwd>
TRAP_COM. : <snmp_pwd>
SYS_NAME. : <snmp_pwd>

where <snmp_pwd> is a password chosen according to the above guidelines. A separate password can be used for each line.

3. Upload the modified configuration file to the print server using the command put config CONFIG. The second argument (CONFIG) must be entered in capitals in order to save the settings permanently.

4. Restart the print server using the command get hardreset.